PRIME
SOFTWARE SOLUTIONS

This Service Level Agreement (the “SLA”) is made pursuant to the Master Service Agreement (“MSA”) executed by and between Prime Software Solutions, LLC (“Provider”) and the signatory to the MSA identified therein as Customer, or the person or entity otherwise receiving Services from Prime (“Customer” or “you”). The SLA shall control to the extent it address an item in a more specific but not contradictory manner as the MSA. To the extent there is any disagreement or ambiguity between the SLA and MSA, the MSA shall control over the SLA. Unless otherwise provided herein, any capitalized term used shall have the meaning as used in the MSA.

1. **Agreement.** Provider agrees to support, maintain, repair or replace Subscription Services.

2. **Provider’s Obligations.**

   (a) Provider shall provide system support for any Service covered in the MSA or applicable SOW so that the Software operates in material conformance with the Documentation. System support will be provided via phone, email, and/or screen sharing session.

   (b) Provider shall provide Customer with updated versions of Software or Subscription Services, such as bug fixes and new releases.

   (c) Provider shall, at its option, repair or replace any Software or component that fails during the term of Customer’s SLA at no cost to Customer, provided that Customer contacts the Provider’s technical support center to report the failure and complies with the MSA and applicable SOW.

   (d) Support@primesoftwaresolutions.com is your designated support email that allows Customers to receive rapid answers to Provider software and service-related questions. Customer can simply email or call (479) 966-9448 24/7 for support. Provider will be available Monday through Friday 8am-5pm Central Standard or Daylight Time. For software support emergencies, call (479) 966-9448 to speak with an on call support agent. If you do not reach anyone, please leave a voicemail and a support agent will contact you asap.

   (e) Provider may use remote access tools to view a specific troubleshooting instance. When accessing the software:

      - Provider will create backup copies of the database and files daily.

- Any requested changes by Customer must be validated by the Provider and approved pursuant to the MSA or applicable SOW.

Provider asks that Customer has either Microsoft Teams, Team Viewer, or similar software to allow for screen sharing with Provider for troubleshooting/support. This will help Provider to witness and diagnose the issue at a much quicker rate.

3. **Security.** Specific measures will be taken by Provider to ensure security of Customer data that is entered into the software.
   (a) All IP address outside of the United States will be blocked to access the server that the system lives on.
   (b) All IP addresses requested by Customer will be blocked upon request.
   (c) Provider can lock down the software to requested IP address by Customer if requested.
   (d) NDAs have been signed by all Provider staff, agents or personnel that will have access to Customer Data.
   (e) Provider has dedicated network engineers whom work daily to ensure software/server security.
   (f) Provider shall not access and shall not permit any access to Customer's systems, databases, data or Confidential Information, whether through Provider's systems or otherwise without Customer's express prior written authorization. All Customer-authorized connectivity to Customer's systems, databases, data or Confidential Information shall be only through Customer's security gateways and firewalls and in compliance with Customer's security policies as may be provided to Provider by Customer from time-to-time. Provider shall be solely responsible for its information technology infrastructure, including all computers, software, databases, electronic systems and networks used by or for Provider to access Customer's systems, database or otherwise in connection with the services and Provider shall prevent unauthorized access to Customer's systems, databases and data through Provider's systems.

4. **Risk Management and Disaster Recovery.** Disaster recovery plan is as follows: If software is destroyed, Provider can recover the software entirely from the last database and files back up that was taken that day. Provider will maintain or cause to be maintained disaster avoidance procedures designed to safeguard the data and Customer's Confidential Information, the availability of the hosted services; maintain a business continuity and disaster recovery plan for any hosted services ("Plan") and implement such Plan for any unplanned interruption of the hosted services. Provider shall actively test (including but not limited to testing with Customer's staffing agency partners and UAT or user acceptance testing), review and update the Plan on at least a quarterly basis using industry best practices. Upon Customer's request, Provider shall provide Customer with copies of all such updates to the Plan. All updates to the Plan shall be subject to the requirements of this Section and upon Customer's request, provide Customer with copies of all reports and summaries resulting from any testing of or pursuant to the Plan after Provider's receipt or preparation thereof.

Security Incident. Provider will inform Customer within 24 hours of detecting any actual or suspected unauthorized access, collection, acquisition, use, transmission, disclosure, corruption or loss of Customer information or data, or breach of any environment containing Customer information or data (each, a "Security Incident"). Provider will remedy each Security Incident in a timely manner and if requested by Customer, provide Customer written details regarding Provider's internal investigation regarding each Security Incident including the date of the breach, the contents of the breach, steps to mitigate the breach and deadlines to resolve the Security Incident. The Parties will reasonably cooperate and work together to form and execute a plan to rectify all confirmed Security Incidents and if requested by Customer, Provider will provide reasonable assistance in obtaining the return of any misappropriated data due to a Security Incident.

Provider Security Policy. Provider will maintain and enforce an information and network security policy for its employees, subcontractors, independent contractors, agents and suppliers that meets the standards set out in Customer's IT Security Policy which may be modified from time to time, including methods to detect and log policy violations. Upon request by Customer, Provider will provide Customer with information on violations of Provider's information and network security policy, even if it does not constitute a Security Incident.

5. **Service Levels**: System Availability

Provider commits to 99.9% Monthly Uptime Percentage based upon 24 hour 7 days a week availability. The percentage of uptime will be calculated by subtracting from 100% the percentage of minutes during a calendar month the system was available subtracting out any scheduled maintenance periods.

Should the Monthly Uptime Percentage fall below 99.9%, Service Credits will be issued based on the following:

Monthly Uptime Percentage	**Service Credit Percentage***
Less than 99.9% but greater than 99.0%	10%
Less than 99.0%	20%

*Credits only apply to monthly Subscription Services fees paid and do not apply to any other monthly fees.

Service Credits apply only against future monthly Subscription Fees due and, once designated by Provider, shall be credited on the next invoice due from Provider to Customer.

SUPPORT

Priority definition

Priority	**Description**
Critical / Urgent	A situation is stopping Customer from running their business.
High	Customer has a serious situation that has no immediate workaround, but does not hinder or preclude daily operation. ***Note: This does not include performance degradation due to Internet connections or inadequate resources to handle network traffic on Customer's end.***
Medium	Customer has an issue causing concern, but not hindering daily operation.
Low	As a general rule, these are situations dealing with cosmetic changes to the Software. Small items and things thought of as "nice to have, but not essential" would be in the category.

Response time commitments are as follows within the priority level:

Priority	**Response Time**	**Support Resolution Time Frame**[1]
Critical/Urgent	Immediate response (i.e., within one hour)	Problem will be worked until solved within 1 calendar day
High	Current day (i.e., within eight business hours)	Within 1 business day
Medium	Current or next day (i.e., within 48 hours)	Within 10 business days
Low	Next day or later (i.e., within 72 hours)	Status will be provided weekly or sooner, issue will be resolved within 20 business days

Support Resolution includes replicating bug conditions and creating documenting the bug with development for resolution. This includes providing workarounds when applicable. Support resolution timeframe does not include the delivery of the code fix. A problem or issue is not resolved until Customer confirms in writing that the problem or issue has been resolved.

Data Backup / Disaster Recovery

- **Full Data Base Backup –** Every night to a second hosting site.
- **Transactional Data Base Backup -** every 2 hours to a second hosting site
- New customer images can quickly be deployed in the event of a disaster.
- Recovery Time Objective (RTO): 4 hours
- Recovery Point Objective (RPO): 2 hours or less